Navigating HIPAA Compliance in Human Subject Research: The Security Rule

The Health Insurance Portability and Accountability Act (HIPAA) aims to safeguard health information and includes provisions under which a covered entity may use or disclose protected health information (PHI) for research purposes. To fulfill the requirements set forth in this act, the Department of Health and Human Service (HHS) constructed the HIPAA Privacy Rule and the HIPAA Security Rule (45 CFR 160 & 45 CFR 164). The Privacy Rule focuses on how PHI is ***utilized*** and the Security Rule focuses on how PHI is ***safeguarded***. The information provided below pertains to the Security Rule. For additional information on the Privacy Rule, see the information available here).

HIPAA Security Rule Basics

Generally, the Security Rule requires covered entities to:

a) Ensure the confidentiality, integrity and availability of all e-PHI that is created, received, maintained or transmitted by the covered entity;
b) Protect against reasonably anticipated threats to the security or integrity of e-PHI;
c) Protect against any reasonably anticipated unauthorized use or disclosure of e-PHI; and
d) Ensure covered entity workforce compliance with the ruling.

The Security Rule further defines several administrative, technical and physical safeguard standards that covered entities must meet, yet the ruling also recognizes the changing landscape of advancing technologies and the range in size, structure and applicability of the ruling to various covered entities. The ruling therefore provides covered entities flexibility in how these standards are implemented. The additional standards, in summary, include:

- Designating a security official for the covered entity;
- Implementing policies and procedures concerning risk analysis and management, sanctions for non-compliance, system activity review, e-PHI access controls, facility access controls, workstation security, device and electronic media security and controls, audit controls, e-PHI transmission security, e-PHI integrity protections, and incident reporting and management; and
- Workforce oversight and training (including security awareness and reminders, protection from malicious software, log-in monitoring, and password management).

The University of Rochester Medical Center (URMC) and Affiliates' Information Security Policies incorporates these standards, as well as other healthcare-focused security standards and best practices (e.g., 21 CFR 11, JCAHO, etc.).

What Do I Need to Do to Comply?

Typically, when study teams consider how they'll safeguard their research data (including any e-PHI) they primarily consider who will have access to the data and where that data will be stored. It's important to recognize however, that because of the nature of the risks related to e-PHI, safeguarding e-PHI extends much

further beyond these two factors; your ability to safeguard e-PHI depends on appropriate day-to-day use of electronic media, both at work and during your personal time.

Key day-to-day expectations and best practices related to the protection of e-PHI, defined in the URMC and Affiliates Information Security Policies, include:

- Keep all information system passwords confidential; DO NOT share passwords.
- Access only job-related information; DO NOT view/alter family member, friend, or acquaintance information.
- Log off or lock (via screen saver password) unattended workstations/computers.
- Encrypt all mobile/portable devices including smartphones, tablets, laptops, digital recorders and flash drives.
- Only store e-PHI via encrypted portable media/laptop/computer, network drive or approved cloud storage (note that Box.com and Microsoft OneDrive are the only approved cloud storage platforms)
- Store portable electronic devices securely when not in use (ideally in a locked cabinet/desk).
- Utilize only authorized photocopiers and other similar technology to reproduce images/documents (e.g., scanners).
- Present research findings in a de-identified format; beware of data that is not categorized as 'identifiable' but may, in combination with other data, become identifiable.
- Inventory all assets to ensure proper tracking/updates (e.g., desktop computers, laptops, tablets, software, smart phones, etc.).
- Dispose of broken or unwanted electronic media/devices via the University's Equipment Recovery Program to ensure retained PHI is rendered unusable, unreadable and undecipherable.
- Beware of phishing! Avoid opening unrecognizable or questionable links/attachments in emails and surfing to unknown websites.
- Only communicate with subjects via e-mail after have provided explicit consent to e-mail communications; encrypt all e-mails containing e-PHI.
- DO NOT send PHI via text message; text messaging is *not* a secure method of communicating with subjects and is generally not permitted.
- DO NOT share PHI on social media.
- Report suspected security incidents to your HIPAA security official.

In addition, if PHI is going to be shared outside of URMC as part of a research study, a security questionnaire should be completed by the recipient organization, and a data transfer agreement may be required.

APPENDIX 1: WHAT IS PHI?

PHI is defined as any individually identifiable information that is created or received by a health care provider that relates to: a) the past, present or future physical or mental health or condition of an individual; b) provision of health care to an individual; or c) the past, present or future payment for the provision of health care to an individual.

APPENDIX 2: WHAT IS A 'COVERED ENTITY'?

A covered entity is defined as a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a standard transaction. The University of Rochester

Medical Center (URMC) & Affiliates covered entity includes over 22 local healthcare facilities/entities (for a full list see the URMC & Affiliates Notice of Privacy Practices). Individuals working in any of the facilities/entities that are part of the URMC & Affiliates covered entity are considered part of the covered entity, regardless of whether they provide direct clinical care to patients (e.g., all individuals working at Eastman Dental, irrespective of their role, are part of the covered entity).

HIPAA requirements only apply to research conducted under a covered entity (e.g., URMC, Highland Hospital, Mt. Hope Family Center, etc.). When all study team members are part of the covered entity, HIPAA compliance is required. Conversely, if *no* members of the study team are affiliated with the covered entity then HIPAA requirements do not apply to the research. If, however, the study team is comprised of *both* members of the covered entity and members who are not part of the covered entity (e.g., River Campus faculty or staff), the entire study team must comply with HIPAA when PHI is collected as part of the research.

ADDITIONAL RESOURCES:

- OHSP Policy 702 HIPAA Privacy Rule
- UR Guideline for Human Subject Research Data Security Requirements
- RSRB Biomedical Consent Template
- OHSP Explains… Assurances, Agreements & Reliance
- OHSP Explains… Coded vs. De-Identified; Anonymized vs. Anonymous
- URMC & Affiliates HIPPA Policies – Information Security Policies
- URMC & Affiliates HIPAA Security FAQs
- HHS HIPAA for Professionals: Summary of the HIPAA Security Rule